Technical Note

ZigBee 网络解析及实现

ZigBee 无线传感网络模块

Date:2009/05/31

工程技术笔记

类别	内容
关键词	ZigBee 技术，ZigBee 网络，ZigBee 解决方案
摘　要	本文简要的介绍了 ZigBee 技术的特点、历史、功能及网络结构，对于标准 ZigBee 网络协议栈做了初步的介绍，在此基础上了解到 ZigBee 市场化进程上遇到的问题，并介绍一种简便易用的 ZigBee 无线应用解决方案。

广州致远电子有限公司

修订历史

版本	日期	原因
V1.00	2009/05/31	创建文档

销售与服务网络（一）

广州周立功单片机发展有限公司

地址：广州市天河北路 689 号光大银行大厦 12 楼 F4
邮编：510630
电话：(020)38730916　38730917　38730972　38730976　38730977
传真：(020)38730925
网址：www.zlgmcu.com

广州专卖店

地址：广州市天河区新赛格电子城 203-204 室
电话：(020)87578634　87569917
传真：(020)87578842

北京周立功

地址：北京市海淀区知春路 113 号银网中心 A 座 1207-1208 室（中发电子市场斜对面）
电话：(010)62536178　62536179　82628073
传真：(010)82614433

杭州周立功

地址：杭州市天目山路 217 号江南电子大厦 502 室
电话：(0571) 28139611　28139612　28139613
28139615　28139616　28139618
传真：(0571) 28139621

深圳周立功

地址：深圳市深南中路 2070 号电子科技大厦 C 座 4 楼 D 室
电话：(0755)83781788（5 线）
传真：(0755)83793285

上海周立功

地址：上海市北京东路 668 号科技京城东座 7E 室
电话：(021)53083452　53083453　53083496
传真：(021)53083491

南京周立功

地址：南京市珠江路 280 号珠江大厦 2006 室
电话：(025)83613221　83613271　83603500
传真：(025)83613271

重庆周立功

地址：重庆市石桥铺科园一路二号大西洋国际大厦（赛格电子市场）1611 室
电话：(023)68796438　68796439
传真：(023)68796439

成都周立功

地址：成都市一环路南二段 1 号数码同人港 401 室（磨子桥立交西北角）
电话：(028)85439836　85437446
传真：(028)85437896

武汉周立功

地址：武汉市洪山区广埠屯珞瑜路 158 号 12128 室（华中电脑数码市场）
电话：(027)87168497　87168297　87168397
传真：(027)87163755

西安办事处

地址：西安市长安北路 54 号太平洋大厦 1201 室
电话：(029)87881296　83063000　87881295
传真：(029)87880865

销售与服务网络（二）

广州致远电子有限公司

地址：广州市天河区车陂路黄洲工业区 3 栋 2 楼
邮编：510660
传真：(020)38601859
网址：www.embedtools.com （嵌入式系统事业部）
www.embedcontrol.com （工控网络事业部）
www.ecardsys.com （楼宇自动化事业部）

技术支持：

CAN-bus：

电话：(020)22644381 22644382 22644253
邮箱：can.support@embedcontrol.com

iCAN 及数据采集：

电话：(020)28872344 22644373
邮箱：ican@embedcontrol.com

MiniARM：

电话：(020)28872684 28267813
邮箱：miniarm.support@embedtools.com

以太网：

电话：(020)22644380 22644385
邮箱：ethernet.support@embedcontrol.com

无线通讯：

电话：(020) 22644386
邮箱：wireless@embedcontrol.com

串行通讯：

电话：(020)28267800 22644385
邮箱：serial@embedcontrol.com

编程器：

电话：(020)22644371
邮箱：programmer@embedtools.com

分析仪器：

电话：(020)22644375 28872624 28872345
邮箱：tools@embedtools.com

ARM 嵌入式系统：

电话：(020)28872347 28872377 22644383 22644384
邮箱：arm.support@zlgmcu.com

楼宇自动化：

电话：(020)22644376 22644389 28267806
邮箱：mjs.support@ecardsys.com
mifare.support@zlgmcu.com

销售：

电话：(020)22644249 22644399 22644372 22644261 28872524
28872342 28872349 28872569 28872573 38601786

维修：

电话：(020)22644245

目录

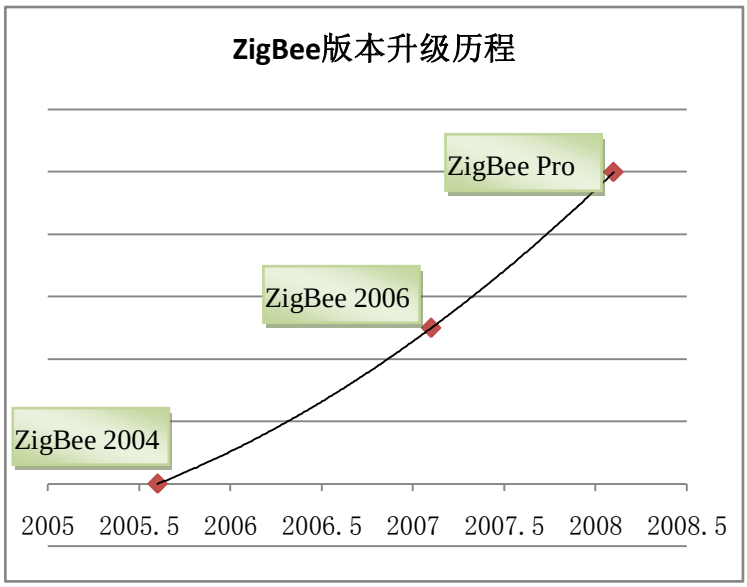
1. ZigBee 网络

1.1 什么是 ZigBee 技术？

ZigBee 名字来源于蜂群使用的赖以生存和发展的通信方式，蜜蜂通过跳 ZigZag 形状的舞蹈来通知发现的新食物源的位置、距离和方向等信息，ZigBee 技术模仿蜜蜂通过跳舞来传递信息的方式，通过相邻网络节点之间信息的接力传递，将一个信息从一个节点传输到远处的另外一个节点。

ZigBee 技术是一种在 900MHz 及 2.4GHz 频段的无线通讯协议，底层基于 IEEE 802.15.4 标准。它的特点是低成本、低功耗（五号电池半年到一年）、低数据率（250Kbps），网络结构优良。

1.2 ZigBee 版本



ZigBee V1.0：这是第一个 ZigBee 标准公开版，于 2005 年 6 月开放下载。

ZigBee V1.1：第二个 ZigBee 标准公开版，于 2007 年 1 月开放下载，又称为 ZigBee 2006。

ZigBee V1.2：第三个 ZigBee 标准公开版，于 2008 年 1 月开放下载，又称为 ZigBee Pro、ZigBee 2007。

1.3 ZigBee 技术特点

- **低成本：**

电源：在低耗电待机模式下，两节普通 5 号干电池可使用 6 个月到 2 年，飞思卡尔最新平台更宣称可以做到待机 20 年。免去了充电或者频繁更换电池的麻烦。这也是 ZigBee 的支持者所一直引以为豪的独特优势;

硬件成本：因为 ZigBee 数据传输速率低，协议简单，所以大大降低了成本。且 ZigBee 协议免收专利费；此外还包括技术发展使得 ZigBee 朝一体化发展，自带 CPU，成本在有望控制在 3 美金左右。

- **经济传输速度：**

本着够用就好的原则，速度在 250Kbps，可以满足它设计用于的家电安防等控制领域，

过高的速率设计带来硬件成本和电源成本的浪费；

- **网络拓扑：**

ZigBee 具有星、树和 mesh 网络结构的能力。ZigBee 设备实际上具有无线网路自愈能力，能简单地覆盖广阔围;每个 ZigBee 网络最多可支持 65535 个设备，也就是说，每个 ZigBee 设备可以与另外 65534 台设备相连接;

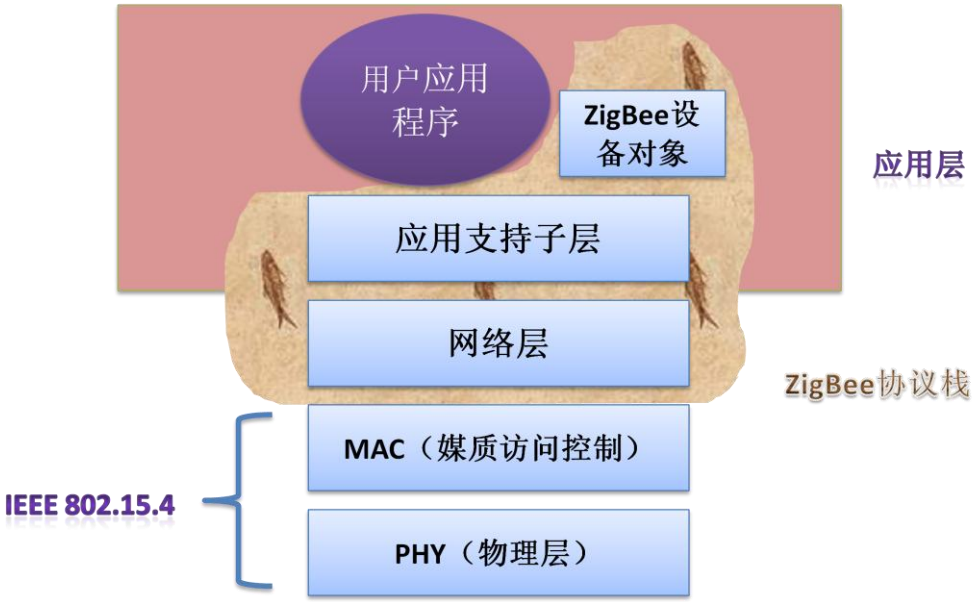
- **行业规范：**

ZigBee 联盟组织花费了大量的精力用于指定 profile 文档，方便 ZigBee 进驻各种应用领域，如灯光控制，只要使用标准的灯光控制的 profile 文件配置即可可不同厂商的产品实现交互，当然前提是这些灯光设备的 ZigBee 模块也是使用标准的 profile，这样智能家居安防监控就可以 DIY 自由组合了。

1.4 网络的特点及优势

1.4.1 协议栈结构

ZigBee 协议栈位于 IEEE802.15.4 物理层及数据链路层规范之上，类似于 TCP/IP 协议栈位于 IEEE 802.3 标准之上一样。



ZigBee 协议栈有“1.75 层”，即“1+0.5+0.25”，1 为完整的网络层(NWL)，0.5 为应用层的下半部分应用支持子层（APSL），0.25 为该层之上的 ZigBee 设备对象（ZDO），应用支持子层对它上一层的协议代码，使用一个字节的端口号（EP，End Point）来区分，类似于 TCP/IP 协议栈的 TCP 端口和 UDP 端口，用来区分不同的服务，而 ZDO 使用端点 0，可用的端口为 1~240，240 之后的端口为协议栈保留端口。

1.4.2 特性

- **接力传送**

ZigBee 网络与有线以太网的结构，在单点传输上，是类似的，在标准介质下，每个网络节点之间的标准距离都不长于 100 米（更长的距离需要增加中继），但是有线以太网的标准介质更为固定，网线的长度就是有效传播范围的尺度，而 ZigBee 无线技术要面临的介质，则包括墙体，人，车辆和建筑物等复杂情况，以至于同样物体不同材料，摆放位置，都会影

响实际的点和点之间有效传播距离，对于有线网络，人们更容易按照电线、电话线等的模式去理解，而无线网络，人们倾向于用手机网络，无线电的模型，因此得出 ZigBee 接力传输的印象，实际上有线网络也是接力传输的。

ZigBee 网络的接力传输，可以解释为，ZigBee 路由节点帮助端节点进行数据转发，从而延伸扩展成为大覆盖面积的无线网络。

- **自组网自恢复**

ZigBee 系驿站位于 IEEE802.15.4 之上，由 ZigBee 联盟指定规范，各大 IT 厂商自己研发 ZigBee 协议栈，ZigBee 规范规定了一系列 ZigBee 网络的组网流程、各种组网行为及帧格式等。

每一个 ZigBee 节点，一旦上电，就会被覆盖范围之内的网络识别，处理其入网申请，成为网络中的一员（如果安全中心允许加入），或者遭到拒绝。

在节点离开网络时（掉电或者更换网络、频段等），网络会检测到并执行删除节点的一系列动作，对于路由节点，该操作非常重要，因为路由节点的退出会改变网络的路由结构，为保障通讯正常或网络损失最小，需要重新组织路由。

- **休眠**

ZigBee 网络中，期望端节点是电池供电的，这样才能更好的体现 ZigBee 技术低功耗的特点，为此，电池供电的节点经常处于休眠状态（多数监控节点只有在出现故障的时候才苏醒报警，故障和意外通常不会每月发生），因此 ZigBee 网络中，除路由节点和协调器节点之外的端节点，通常会被置于休眠状态，可有传感器唤醒，或者路由节点唤醒。

因此 ZigBee 网络还存在“端节点”处于休眠态该如何处理数据包的规则。

2. ZigBee 组网

ZigBee 标准网络定义了三种类型（ZigBee device type），对这三种角色的行为的说明，是了解整个协议栈运作的很好切入点。

2.1 角色介绍

2.1.1 协作员（coordinator）

协调器负责启动整个网络。它也是网络的第一个设备。协调器选择一个信道和一个网络 ID(也称之为 PAN ID，即 Personal Area Network ID)，随后启动整个网络。

协调器也可以用来协助建立网络中安全层和应用层的绑定(bindings)。注意，协调器的角色主要涉及网络的启动和配置。

2.1.2 路由（router）

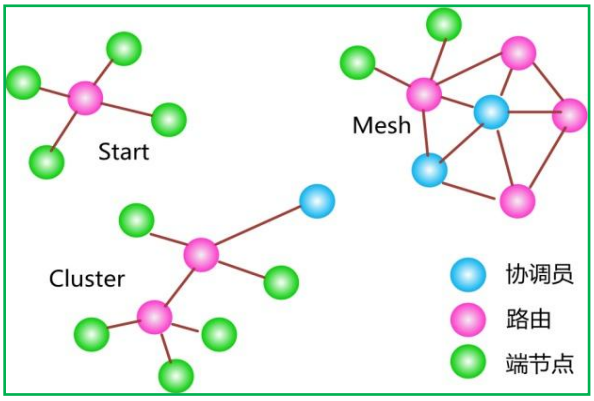
路由器的功能主要是：允许其他设备加入网络，多跳路由和协助它自己的由电池供电的儿子终端设备的通讯。

2.1.3 端节点（end device）

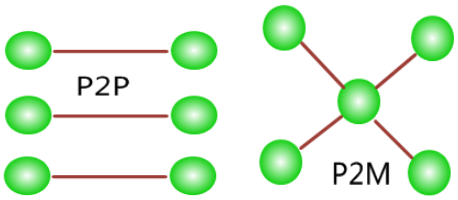
终端设备没有特定的维持网络结构的责任，它可以睡眠或者唤醒，因此它可以是一个电池供电设备。

2.2 网络拓扑

ZigBee 网络有以下三种组网方式，星型网、簇型网和网状网。其中红色和蓝色的节点（路由节点和协调员节点）才具有转发功能，由他们构建网络框架。



另外，直接使用 IEEE 802.15.4 底层的还有以下两种方式，即点对点模式（P2P）和点对多点(P2M)模式，这在实际应用中使用比较广泛，因为只需要点对点通讯，程序开发简单。



2.3 美中不足

ZigBee 技术先进，在嵌入式技术发达的国家，应用发展的势头如星火燎原，但是在走

入技术相对弱一些的区域，先进有时意味着复杂和不可把握，自组网自恢复是 ZigBee 网络的一大特色，为网络的健壮性和便捷性提供了保障，但是完善的机制往往会变得过于复杂，分析起来非常困难，需要对整个协议栈非常了解才能判断情况。

关于源代码，TI 虽然公布了自己 ZigBee pro 协议栈的代码，但是本身协议栈的流程和状态图就很复杂，理解及开发的难度很大。

另外，其睡眠机制也存在一定的可优化之处，路由节点在标准协议中通常要求长期供电，不能使用电池，这给网络部署带来一定的障碍。

以上的问题都是用户在使用 ZigBee 技术不容回避的问题，如果没有找到合适的方案，轻易不要挑战这些技术难点，开销是巨大的。

3. ZigBee 协议栈实用技术

技术的市场化，一个重要的特点，在于降低技术本身的使用难度，各自做自己擅长的事情，大家才能方便的用起新技术，走完技术发展的最后一站，因此，IT 公司的技术人员总是不断的努力推出满足应用需求的产品和服务，针对 ZigBee 标准协议栈的开发难度和功耗问题，目前已经取得不少的进步。

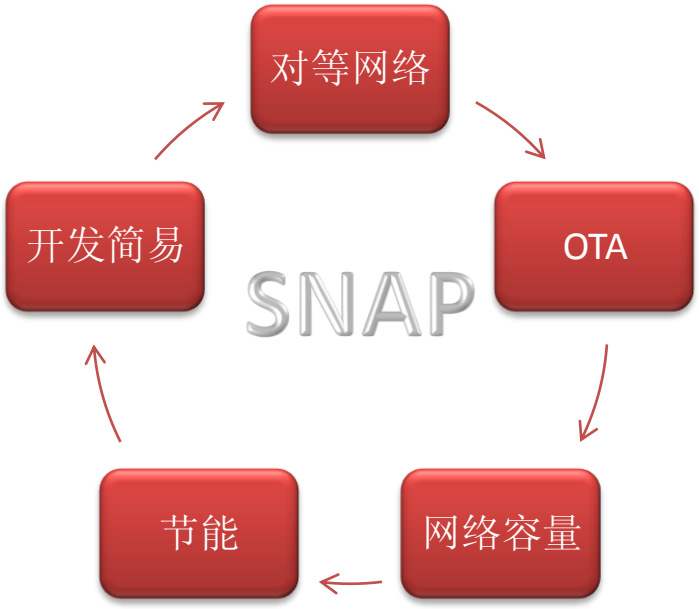
技术的更新和发展，不光是实验室里的研究，也包括来自更大技术厂商应用经验的积累，国际标准的制定也是搜集借鉴了市场上不同技术公司的优点，集思广益，不断更新。

以下介绍一个商用的 ZigBee 协议栈方案。

3.1 什么是 SNAP

SNAP 网络协议是一款由 Synapse 公司开发的无线 mesh 网络协议，Synapse 公司是国际上专业的无线网状网软硬件解决方案提供商，SNAP 为复杂的 ZigBee 网络提供一个简单、可靠、智能的完整组网方案，同时，因为使用“对等网络”概念，功耗优化明显，冗余性能优异。

3.2 SNAP 网络原理



SNAP 网络是具有以下特点的网络：

3.2.1 对等网络

在 IT 领域，过去是服务器和终端的概念，终端只负责输入输出，计算全部在服务器端完成，之后的 CS（客户机服务器模式），终端具备简单的处理能力，以客户机模式和服务器进行交互，随着客户机计算能力的增强，更多的计算任务可以由客户机来完成，PC 机的配置越来越强，服务器的负担逐渐转向个人电脑，“云计算”的思路正一步步的实现。

从下载的角度来讲，过去往往是个人从网站上下载文件（文档，音乐及视频等）或

应用程序，而之后出现的 P2P 对等网络，以及 BT 软件，开启了对等网络的时代，逐渐的模糊了服务器的概念。

SNAP 同样使用的是对等网络，所有的节点都是路由节点，组网时，无“加入网络”过程，无中心节点，无需预先构架网络拓扑。

3.2.2 网络容量

由于 SNAP 使用了 24 位（3 字节）网络地址，因此理论上单个网络可以拥有 16M 个节点，网络使用 16 位 （2 字节）地址，因此支持 64K 个网络。

3.2.3 节能

SNAP 网络支持一种“集体协议睡眠”方式，由附近的节点选举产生一个领导节点（或者 Python 脚本指定），根据领导节点知道的信息，向周围节点发出类似“睡眠 100ms”的命令，然后所有节点（包括他自己），都进入睡眠模式，醒来之后“有事禀报，无事退朝”，继续进入睡眠，因此，SNAP 网络是一个“贪睡虫网络”。

3.2.4 开发简易

由于使用了 Python 虚拟机，因此底层能用的硬件和功能都封装成函数，通常只需要十几行代码完成复杂应用 。

3.2.5 Updata OTA

OTA 是 On The Air 的缩写，在介绍空中升级之前，我们先来了解一下实现该技术的一些知识。

OTA 使用的是先进的 Python 语言，Python 是一种面向对象的解释性的计算机程序设计语言， 也是一种功能强大而完善的通用型语言，类似于 java 但是更简单，它在虚拟机上运行，应用程序是有 Python 脚本来完成。

使用该技术的一个特点是，可以在应用程序开发的同时，部署 ZigBee 硬件节点，部署完成，程序也同时完成，只需要使用连接电脑的网关节点进行空中升级即可，程序的更改非常方便。

应用 Python 的工程师比较喜欢“注入代码”这个词汇，因为一个端节点的功能及行为，都是可以通过在连接网关的 PC 上编写，然后无线下载到目标设备里，之所以使用“注入”而不使用“下载”，因为 Python 脚本是设备全部代码的一部分（下层的虚拟机和底层驱动是不会被擦除的），类似无线的 IAP。

在城市照明的路灯项目中，利用 Python 技术实现的 Update OTA 可以先安装 ZigBee 模块，然后在路灯下面上载（注入）控制程序，软硬同时开工。以后如果升级，也可以同样站在路上操作即可，并不需要取下来（这样做的成本是很高的）。

3.3 应用

SNAP 网络已经在国外有很多成熟的应用，路灯网络（几千个节点一个网络），农田环境监测，机场雷电监测，公园场景音响，煤矿个人安全保障系统等等。